10/029,349

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	218	380/285	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/11 14:50
L2	5747	380/282 or 380/259 or 380/203 or 713/193 or 713/167 or 713/165 or 713/194 or 713/171 or 705/59 or 380/29 or 380/42 or 380/277 or 726/1	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/11 15:01
L3	596	license and attributes and "public key" and signature and decrypt$4 and "private key"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/11 15:30
L4	5	3 and 2 and 1	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/11 15:27
L5	14	hurst.inv. and leon	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/11 15:27
L6	12	durand.inv. and julian	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/11 15:28
L7	8	wilkinson.inv. and jeffery	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/11 15:28
L8	0	tampere.inv. and muligan	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/11 15:29

L9	78	mulligan.inv. and michael	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/11 15:30
L10	0	9 and 7 and 6 and 1	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/11 15:30
L11	0	9 and 7 and 6 and 5	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/11 15:30
L12	0	license.clm. and attributes.clm. and "public key".clm. and signature.clm. and decrypt$4.clm. and "private key".clm.	USPAT	OR	OFF	2006/02/11 15:31

Subscribe (Full Service)   Register (Limited Service, Free)   Login

Search: ⦿ The ACM Digital Library   ⦿ The Guide

license and attributes and "public key" and signature and decr

THE ACM DIGITAL LIBRARY

☞ Feedback Report a problem Satisfaction survey

Terms used **license** and **attributes** and **public key** and **signature** and **decrypt$4** and **private key**

Found **2,929** of **169,866**

| Sort results by | relevance ▾ |
| Display results | expanded form ▾ |

❖ Save results to a Binder

🗐 Search Tips

☐ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200

Result page: **1** 2 3 4 5 6 7 8 9 10   next

Best 200 shown

Relevance scale ☐▭▬◼◼

1 **Multi-agent systems and social behavior: A user-centric anonymous authorisation framework in e-commerce environment**
Richard Au, Harikrishna Vasanta, Kim-Kwang Raymond Choo, Mark Looi
March 2004 **Proceedings of the 6th international conference on Electronic commerce ICEC '04**
Publisher: ACM Press
Full text available: 📄 pdf(291.06 KB)   Additional Information: full citation, abstract, references

A novel user-centric authorisation framework suitable for e-commerce in an open environment is proposed. The credential-based approach allows a user to gain access rights anonymously from various service providers who may not have pre-existing relationships. Trust establishment is achieved by making use of referrals from external third parties in the form of *Anonymous Attribute Certificates.* The concepts of *One-task Authorisation Key* and *Binding Signature* are proposed to fac ...

2 **Authentication and signature schemes: On the performance, feasibility, and use of forward-secure signatures**
Eric Cronin, Sugih Jamin, Tal Malkin, Patrick McDaniel
October 2003 **Proceedings of the 10th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: 📄 pdf(386.51 KB)   Additional Information: full citation, abstract, references, index terms

Forward-secure signatures (FSSs) have recently received much attention from the cryptographic theory community as a potentially realistic way to mitigate many of the difficulties digital signatures face with key exposure. However, no previous works have explored the practical performance of these proposed constructions in real-world applications, nor have they compared FSS to traditional, non-forward-secure, signatures in a non-asymptotic way.We present an empirical evaluation of several FSS sch ...

Keywords: digital signatures, forward-secure signatures

3 **DRM experience: Digital rights management in a 3G mobile phone and beyond**
Thomas S. Messerges, Ezzat A. Dabbish
October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**

Publisher: ACM Press

Full text available: pdf(306.59 KB)   Additional Information: full citation, abstract, references, citings, index terms

In this paper we examine how copyright protection of digital items can be securely managed in a 3G mobile phone and other devices. First, the basic concepts, strategies, and requirements for digital rights management are reviewed. Next, a framework for protecting digital content in the embedded environment of a mobile phone is proposed and the elements in this system are defined. The means to enforce security in this system are described and a novel "Family Domain" approach to content management ...

Keywords: MPEG-21, copyright protection, cryptography, digital content, digital rights management, embedded system, key management, mobile phone, open mobile alliance, security

4 Technologies for repository interoperation and access control

Shirley Browne, Jack Dongarra, Jeff Horner, Paul McMahan, Scott Wells
May 1998 **Proceedings of the third ACM conference on Digital libraries**
Publisher: ACM Press
Full text available: pdf(1.14 MB)   Additional Information: full citation, references, citings, index terms

5 Separating key management from file system security

David Mazières, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchel
December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles SOSP '99**, Volume 33 Issue 5
Publisher: ACM Press

Full text available: pdf(1.77 MB)   Additional Information: full citation, abstract, references, citings, index terms

No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security at a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use. We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal ...

6 Mobile computing and applications (MCA): Delivering Attribute Certificates over GPRS

Georgios Kambourakis, Angelos Rouskas, Stefanos Gritzalis
March 2004 **Proceedings of the 2004 ACM symposium on Applied computing**
Publisher: ACM Press
Full text available: pdf(182.76 KB)   Additional Information: full citation, abstract, references, index terms

Attribute Certificates (ACs) have been developed and standardized by the ANSI X9 committee as an alternative and better approach, to X.509 public key certificates, for carrying authorization information. Attribute Authorities (AA) bind the characteristics of an entity (called attributes) to that entity by signing the appropriate AC. Therefore, ACs can be used for controlling access to system resources and employing role-based authorization and access controls policies accordingly. Although ACs a ...

Keywords: GPRS, PKI, UMTS, attribute certificates, performance evaluation

7

7   A security architecture for fault-tolerant systems

Michael K. Reiter, Kenneth P. Birman, Robbert van Renesse
November 1994 **ACM Transactions on Computer Systems (TOCS)**, Volume 12 Issue 4
Publisher: ACM Press

Full text available: pdf(2.50 MB)   Additional Information: full citation, abstract, references, citings, index terms, review

Process groups are a common abstraction for fault-tolerant computing in distributed systems. We present a security architecture that extends the process group into a security abstraction. Integral parts of this architecture are services that securely and fault tolerantly support cryptographic key distribution. Using replication only when necessary, and introducing novel replication techniques when it was necessary, we have constructed these services both to be easily defensible against atta ...

Keywords: key distribution, multicast, process groups

8   Credentials: Concealing complex policies with hidden credentials

Robert W. Bradshaw, Jason E. Holt, Kent E. Seamons
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security**
Publisher: ACM Press

Full text available: pdf(219.13 KB)   Additional Information: full citation, abstract, references, index terms

Hidden credentials are useful in protecting sensitive resource requests, resources, policies, and credentials. We propose a significant performance improvement when implementing hidden credentials using Boneh/Franklin Identity Based Encryption. We also propose a substantially improved secret splitting scheme for enforcing complex policies, and show how it improves concealment of policies from nonsatisfying recipients.

Keywords: authentication, credentials, identity based encryption, privacy, secret sharing, trust negotiation

9   Cryptographic protocols: Design and implementation of the *idemix* anonymous credential system

Jan Camenisch, Els Van Herreweghen
November 2002 **Proceedings of the 9th ACM conference on Computer and communications security**
Publisher: ACM Press

Full text available: pdf(1.09 MB)   Additional Information: full citation, abstract, references, citings, index terms

Anonymous credential systems [8, 9, 12, 24] allow anonymous yet authenticated and accountable transactions between users and service providers. As such, they represent a powerful technique for protecting users' privacy when conducting Internet transactions. In this paper, we describe the design and implementation of an anonymous credential system based on the protocols developed by [6]. The system is based on new high-level primitives and interfaces allowing for easy integration into access cont ...

Keywords: anonymous credential systems, cryptographic protocols, privacy

10   Authentication metric analysis and design
Michael K. Reiter, Stuart G. Stubblebine

May 1999 **ACM Transactions on Information and System Security (TISSEC),** Volume 2
Issue 2
Publisher: ACM Press

Full text available: pdf(154.45 KB)   Additional Information: full citation, abstract, references, citings, index terms, review

Authentication using a path of trusted intermediaries, each able to authenicate the next in the path, is a well-known technique for authenicating entities in a large-scale system. Recent work has extended this technique to include multiple paths in an effort to bolster authentication, but the success of this approach may be unclear in the face of intersecting paths, ambiguities in the meaning of certificates, and interdependencies in the use of different keys. Thus, several authors have pro ...

Keywords: metrics of authentication, public key infrastructure

11 Verification and security: Policy-hiding access control in open environment

Jiangtao Li, Ninghui Li
July 2005 **Proceedings of the twenty-fourth annual ACM SIGACT-SIGOPS symposium on Principles of distributed computing PODC '05**
Publisher: ACM Press

Full text available: pdf(247.72 KB)   Additional Information: full citation, abstract, references, index terms

In trust management and attribute-based access control systems, access control decisions are based on the attributes (rather than the identity) of the requester: Access is granted if Alice's attributes in her certificates satisfy Bob's access control policy. In this paper, we develop a policy-hiding access control scheme that protects both sensitive attributes and sensitive policies. That is, Bob can decide whether Alice's certified attribute values satisfy Bob's policy, without Bob learning any ...

Keywords: access control, automated trust negotiation, cryptographic commitment, cryptographic protocol, digital credentials, evaluation, privacy, secure function

12 DRM usability and legal issues: Import/export in digital rights management

Reihaneh Safavi-Naini, Nicholas Paul Sheppard, Takeyuki Uehara
October 2004 **Proceedings of the 4th ACM workshop on Digital rights management**
Publisher: ACM Press

Full text available: pdf(211.60 KB)   Additional Information: full citation, abstract, references, index terms

The inherently controlled nature of digital rights management systems does little to promote inter-operability of systems provided by different vendors. In this paper, we consider import and export functionality by which multimedia protected by one digital rights management regime can be made available to a multimedia device that supports a different digital rights management regime, without compromising the protection afforded to the content under the original regime. We first identify speci ...

Keywords: digital rights management, export, import, inter-operability

13 Digital signatures: can they be accepted as legal signatures in EDI?

Patrick W. Brown
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**
Publisher: ACM Press

Full text available: pdf(809.34 KB)   Additional Information: full citation, abstract, references, citings, index terms

Digital Signature (DS) technology may be employed to produce legally enforceable signatures in Electronic Data Interchange (EDI) among computer users within the same general guidelines and requirements as those developed for handwritten signatures on paper. Digital signature technology promises assurance at least equal to written signatures. From a legal standpoint, this assurance remains to be tested in the evidentiary process. Business policies for organizational use of this technology ar ...

Keywords: EDI, cryptography, digital signatures, distributed systems, law

14 Email and security: How to make secure email easier to use

Simson L. Garfinkel, David Margrave, Jeffrey I. Schiller, Erik Nordlander, Robert C. Miller
April 2005 **Proceedings of the SIGCHI conference on Human factors in computing systems**
Publisher: ACM Press
Full text available: pdf(419.10 KB)   Additional Information: full citation, abstract, references, index terms

Cryptographically protected email has a justly deserved reputation of being difficult to use. Based on an analysis of the PEM, PGP and S/MIME standards and a survey of 470 merchants who sell products on Amazon.com, we argue that the vast majority of Internet users can start enjoying digitally signed email today. We present suggestions for the use of digitally signed mail in e-commerce and simple modifications to webmail systems that would significantly increase integrity, privacy and authorship ...

Keywords: e-commerce, user interaction design, user studies

15 Trust management: Preventing attribute information leakage in automated trust negotiation

Keith Irwin, Ting Yu
November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**
Publisher: ACM Press
Full text available: pdf(217.27 KB)   Additional Information: full citation, abstract, references, index terms

Automated trust negotiation is an approach which establishes trust between strangers through the bilateral, iterative disclosure of digital credentials. Sensitive credentials are protected by access control policies which may also be communicated to the other party. Ideally, sensitive information should not be known by others unless its access control policy has been satisfied. However, due to bilateral information exchange, information may flow to others in a variety of forms, many of which can ...

Keywords: attribute-based access control, privacy, trust negotiation

16 The emerging law of international electronic commerce: recent work by UNCITRAL

Henry Deeb Gabriel
September 2003 **Proceedings of the 5th international conference on Electronic commerce ICEC '03**
Publisher: ACM Press
Full text available: pdf(148.85 KB)   Additional Information: full citation, abstract, references, index terms

This paper describes the minimal aspects of any law intended to govern electronic commerce, and discusses the recent attempts by the United Nations Commission on International Trade Law to create a legal framework for electronic commerce. Electronic commerce laws recognize the validity of electronic records, signatures and contracts without changing the underlying substantive law of contracts. The UNCITRAL approach to

electronic commerce legislation is based on the "functional-equivalent" approa ...

Keywords: contract, functional equivalence, media neutrality

17 APL.NET encryption HOWTO

Vladimir Kutinsky
March 2004 **ACM SIGAPL APL Quote Quad**, Volume 34 Issue 2
Publisher: ACM Press
Full text available: pdf(233.13 KB)   Additional Information: full citation, abstract, references

The article outlines the key points of building a Dyalog APL interface to the GNU Privacy Guard (GnuPG), a tool for cryptographic privacy and authentication. The main purpose of the interface is to use the GnuPG's functionality to encrypt data and create digital signatures directly from APL programs. The article briefly describes .NET classes that form the core of the interface and provide effective means to manage processes running on a computer. It also contains a number of examples demonstrat ...

18 Random oracles are practical: a paradigm for designing efficient protocols

Mihir Bellare, Phillip Rogaway
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**
Publisher: ACM Press

Full text available: pdf(1.17 MB)   Additional Information: full citation, abstract, references, citings, index terms

We argue that the random oracle model—where all parties have access to a public random oracle—provides a bridge between cryptographic theory and cryptographic practice. In the paradigm we suggest, a practical protocol P is produced by first devising and proving correct a protocol PR for the random oracle model, and then replacing oracle accesses by the computation of an "appropriately chosen" function h

19 Internet printing protocol (IPP) encoding and transport

Carl Kugler, Harry Lewis
December 1998 **StandardView**, Volume 6 Issue 4
Publisher: ACM Press
Full text available: pdf(399.88 KB)   Additional Information: full citation, references

20 Identification control: Public key distribution through "cryptoIDs"

Trevor Perrin
August 2003 **Proceedings of the 2003 workshop on New security paradigms**
Publisher: ACM Press
Full text available: pdf(1.51 MB)   Additional Information: full citation, abstract, references, index terms

In this paper, we argue that person-to-person key distribution is best accomplished with a key-centric approach, instead of PKI: users should distribute public key fingerprints in the same way they distribute phone numbers, postal addresses, and the like. To make this work, fingerprints need to be *small*, so users can handle them easily; *multipurpose*, so only a single fingerprint is needed for each user; and *long-lived*, so fingerprints don't have to be frequently redistribute ...

Keywords: cryptoIDs, fingerprints, key distribution, key management, public key infrastructure